TASK-1

TOP 10 NOTORIOUS HACKERS OF ALL TIME IN THIS INTERNET WORLD

KEVIN MITNIK

Kevin Mitnick was a notorious hacker in the 1980s and 1990s but has since turned his life around. He's now a cybersecurity consultant and author, helping organizations stay secure. He no longer engages in hacking activities.

Kevin Mitnick was a black hat hacker during his hacking activities in the past. Black hat hackers engage in illegal and malicious activities, such as breaking into computer systems without authorization. However, as mentioned earlier, he has since become an ethical hacker (often referred to as a white hat hacker) and now works to help organizations improve their cybersecurity defenses.

ANONYMOUS

Anonymous is not the name of a single individual but rather a loosely organized and decentralized collective of activists and hackers. Therefore, it's not accurate to refer to Anonymous as a single hacker or to assign a specific type of hacker label to them. Instead, Anonymous is a group of individuals with diverse motivations, and their actions can range from peaceful online protests and activism to more controversial or illegal hacking activities.

Some members of Anonymous may engage in hacking activities to further their causes, which could include actions that some might consider "black hat" hacking, while others may focus on using their skills for "gray hat" or even "white hat" purposes, such as exposing wrongdoing or advocating for free speech and privacy rights.

It's important to understand that Anonymous lacks a centralized leadership structure, and individuals who claim to be part of Anonymous may have different goals and motivations. As a result, it's difficult to categorize the entire collective under a single label, as their activities and intentions can vary widely.

ADRIAN LAMO

Adrian Lamo was a computer hacker best known for his involvement in the case of Chelsea Manning, formerly known as Bradley Manning. Lamo reported Manning to the authorities after Manning confided in him about leaking classified military documents to WikiLeaks. Lamo's actions in this case sparked controversy and debate.

Adrian Lamo, the computer hacker and security analyst, would be best classified as a "gray hat" hacker during his active hacking days. Gray hat hackers are individuals who operate in a somewhat ambiguous ethical space between black hat (malicious hackers) and white hat (ethical hackers). Lamo was known for hacking into systems but often did so with the intention of exposing security vulnerabilities and notifying the affected parties rather than causing harm or personal gain. His actions, including reporting Chelsea Manning's unauthorized disclosure of classified documents, reflect a mix of ethical motivations, making him a gray hat hacker.

ALBERT GONZALEZ

Albert Gonzalez (born 1981) is an American computer hacker, computer criminal and police informer,[who is accused of masterminding the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from 2005 to 2007, the biggest such fraud in history. Gonzalez and his accomplices used SQL injection to deploy backdoors on several corporate systems in order to launch packet sniffing (specifically, ARP Spoofing) attacks which allowed him to steal computer data from internal corporate networks.

He was a black hacker.

Matthew Bevan and Richard Pryce

Matthew Bevan and Richard Pryce are individuals known for their involvement in hacking activities during the 1990s.

Matthew Bevan, a British hacker, gained notoriety for allegedly breaking into U.S. military computer systems in the early 1990s. He was accused of hacking into computer systems belonging to the U.S. Air Force and NASA, among others. His activities raised concerns about the security of military and government computer networks. Bevan's actions led to an investigation, but he denied any malicious intent and claimed that he was merely exploring computer systems out of curiosity.

Richard Pryce, also known as "Datastream Cowboy," was another British hacker active during the 1990s. Pryce was involved in hacking into various U.S. government and military systems, including those belonging to the U.S. Navy. Like Bevan, Pryce's activities raised significant security concerns.

Matthew Bevan and Richard Pryce are often classified as "black hat" hackers. They engaged in unauthorized hacking activities, including breaking into computer systems without permission, which is a defining characteristic of black hat hackers. While their motivations may have been exploratory or curiosity-driven, their actions were illegal and did not align with the ethical and legal standards typically associated with white hat hackers or cybersecurity professionals.

Jeanson James Ancheta

Jeanson James Ancheta, also known as Jeanson Wong, was a cybercriminal known for creating and controlling a botnet, a network of infected computers. He used this botnet for various malicious activities, including DDoS attacks and spreading adware. He was arrested in 2006 and sentenced to prison for his illegal actions.

Jeanson James Ancheta was primarily a black hat hacker. His activities involved creating and using a botnet for malicious purposes, such as conducting distributed denial-of-service (DDoS) attacks and spreading adware without authorization. Black hat hackers engage in illegal and harmful activities in the world of cybersecurity.

Michael Calce

Michael Calce, also known as "Mafiaboy," is a Canadian hacker who gained notoriety in 2000 for launching a series of high-profile DDoS (Distributed Denial of Service) attacks against major websites, including Yahoo, Amazon, eBay, and CNN. He was a teenager at the time of these attacks and was responsible for significant disruptions to these online services.

Calce's actions were illegal, and he was eventually arrested and convicted for his cybercrimes. His case highlighted the potential damage that DDoS attacks can inflict on internet infrastructure and raised awareness about the need for improved cybersecurity measures.

Since his arrest and conviction, Calce has expressed remorse for his actions and has become an advocate for cybersecurity awareness, cautioning against engaging in illegal hacking activities.

Michael Calce, also known as "Mafiaboy," would typically be classified as a black hat hacker. He engaged in illegal and malicious activities by launching DDoS attacks against major websites, causing significant disruptions. Black hat hackers are individuals who engage in hacking activities for personal gain, harm, or illegal purposes, which was the case with Calce's actions.

JONATHAN JAMES

Jonathan James, also known as "c0mrade," was an American hacker known for his involvement in various cybercrimes. In 2000, at the age of 16, he became the youngest person to be convicted of a cybercrime in the United States. James was responsible for hacking into several high-profile systems, including NASA's computers, from which he stole sensitive software and data.

His actions were categorized as black hat hacking because they involved unauthorized intrusions and data theft. Unfortunately, James faced legal consequences for his activities, and in 2008, he tragically committed suicide. His case serves as a reminder of the serious legal and ethical implications associated with hacking and cybercrimes.

Jonathan James was primarily a black hat hacker. His hacking activities involved unauthorized intrusions into computer systems, including NASA's, and the theft of sensitive software and data. Black hat hackers engage in hacking for personal gain, malicious intent, or illegal purposes, which aligns with James's actions.

ASTRA

This hacker differs from the others on this list in that he has never been publicly identified. However, according to the Daily Mail, some information has been released about ASTRA. Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world. His hacking cost the Dassault Group $360 million in damages. No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.